(12) UK Patent Application (19) GB (11) 2 261 579 (13) A

(43) Date of printing by UK Office 19.05.1993

(21) Application No 9226468.8

(22) Date of filing 18.07.1991

(30) Priority data
(31) 556890 (32) 23.07.1990 (33) US

(86) International application data
PCT/US91/05078 En 18.07.1991

(87) International publication data
WO92/02087 En 06.02.1992

(71) Applicant
Ericsson Ge Mobile Communications Inc

(Incorporated in the USA - Delaware)

1 Triangle Drive, Research Triangle Park, NC 27709, United States of America

(72) Inventor
Paul Wilkinson Dent

(74) Agent and/or Address for Service
Haseltine Lake & Co
Hazlitt House, 28 Southampton Buildings, Chancery Lane, London, WC2A 1AT, United Kingdom

(51) INT CL[5]
H04L 9/32

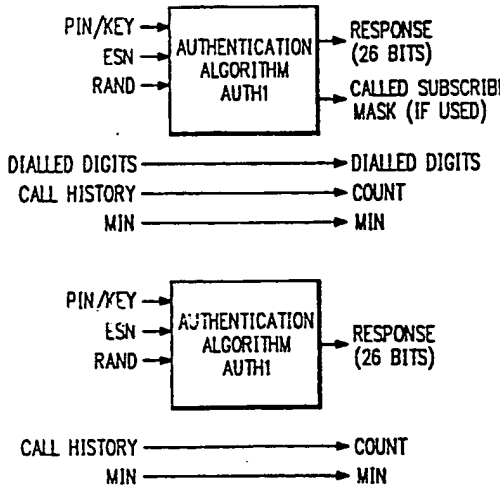
(52) UK CL (Edition L)
H4P PDCSA
U1S S2204 S2213

(56) Documents cited by ISA
US 4914696 A US 4876740 A US 4827507 A
US 4549308 A

(58) Field of search by ISA
US CL. 380/21,23,28,43,44,46,47,48,49,50, 455/33, 375/107,110,112. 370/103,105,107, 379/59,60.

(54) Authentication system for digital cellular communications

(57) A system for the authentication of mobile stations and base stations in a cellular communications network. The system includes an algorithm which generates not only a key dependent response to a random challenge, but also a temporary conversation key or call variable which may be used to encipher traffic in the network. To protect against clones in the network, the algorithm uses a rolling key which contains historical information. A bilateral authentication procedure may be used to update the rolling key and to generate a new conversation key.



GB 2 261 579 A

(12) UK Patent Application (19) GB (11) 2 296 413 (13) A

(43) Date of Printing by UK Office 26.06.1996

(21) Application No 9604489.6

(22) Date of Filing 05.07.1995

(30) Priority Data
(31) 08270564 (32) 05.07.1994 (33) US

(86) International Application Data
PCT/US95/08421 En 05.07.1995

(87) International Publication Data
WO96/01536 En 18.01.1996

(71) Applicant(s)
Motorola Inc

(Incorporated in USA - Delaware)

Corporate Offices, 1303 East Algonquin Road, Schaumburg, Illinois 60196, United States of America

(72) Inventor(s)
Jennifer Ann Pierce
Louis David Finkelstein
Peter B Brown
Jay R Krebs

(51) INT CL[6]
H04L 9/32 9/16 9/22

(52) UK CL (Edition O)
H4P PDCSA

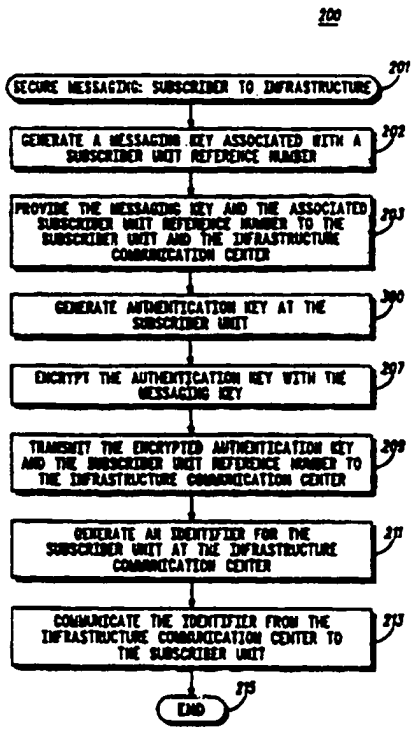
(56) Documents Cited by ISA
US 5410602 A US 5392356 A US 5341427 A
US 5301247 A US 5249230 A US 5227613 A
US 5196840 A US 5077790 A US 4876716 A
US 4268715 A

(58) Field of Search by ISA
INT CL[6] H04L 9/16 9/22 9/32
U.S.: 380/21,23,44

(74) Agent and/or Address for Service
Sarah J Spaulding
Motorola Limited, European Intellectual Property Operation, Midpoint, Alencon Link, BASINGSTOKE, Hampshire, RG21 7PL, United Kingdom

(54) **A method of messaging in a communciation system**

(57) A communication system (100) employs a method of messaging between a subscriber unit (105) and an infrastructure communication center (101). A messaging key associated with a subscriber unit reference number is provided (203, 403) to the subscriber unit (105) and to the infrastructure communication center (101). An authentication key and/or an identifier for the subscriber unit (105) is then produced (300, 407) by either the subscriber unit (105) or the infrastructure communication center (101). The authentication key and/or the identifier is encrypted (207, 413) with the messaging key and is subsequently communicated (209, 415) between the subscriber unit (105) and the infrastructure communication center (101).



GB 2 296 413 A